UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,479	12/07/2004	Franciscus Lucas Antonius Johannes Kamperman	2069.057US1	6117

21186 7590 03/04/2008
SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER
CHAI, LONGBIT

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
03/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

	Application No.	**Applicant(s)**
	10/517,479	KAMPERMAN ET AL.
	Examiner	**Art Unit**
	Longbit Chai	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 October 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *10/12/2006*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 12/7/2004 but has a foreign priority application filed on 6/12/2002.

Claim Objections

2. Claims 2 – 7 are objected to because of the following informalities: “A method” should be “The method”.

3. Claims 9 – 12 are objected to because of the following informalities: “A conditional access apparatus” should be “The conditional access apparatus”.

4. Claim 8 is objected to because of the following informalities: storage means should use the typical format “means for” because the word "means" is preceded by the word “storage” in an attempt to use a "means" clause served as a means for performing a specified function.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1 – 5 and 8 – 12 are rejected under 35 U.S.C. 102(b) as being anticipated by Kamperman (U.S. Patent 5,991,400).

As per claim 1, Kamperman teaches a method of processing a broadcast data stream that contains a stream of encrypted data and a stream of messages (Kamperman : Column 1 Line 55 – Column 2 Line 3), data in successive segments of the stream of encrypted data being decryptable with successive decryption information from the messages (Kamperman : Column 1 Line 55 – 67: ECM messages), the method comprising:

storing the stream of encrypted data (Kamperman : Column 2 Line 61 – 62);

storing items with decryption information for the encrypted data independently retrievable from the stream (Kamperman : Column 2 Line 59 – 61, Column 1 Line 55 – 67 and Column 4 Line 41 – 59: ECM message embedded / multiplexed with the encrypted / scrambled data that contains control word (CW) (i.e. decryption information) corresponding to reception of the data stream during each respective 10 seconds block of data);

storing synchronization information linking respective points in the stored stream of encrypted data to respective ones of the items with decryption information (Kamperman : Column 8 Line 42 – 51 and Column 7 Line 2 – 5: the time-stamped information is qualified as a synchronization information that determines the validity time period of the ECM control word (i.e. decryption information) that is used to successfully decode the encrypted data);

replaying a stored part of the stream of encrypted data (Kamperman : Column 5 Line 55 – 60: a play-back recorder);

retrieving the items with decryption information for the points in said stored part during said replaying (Kamperman : Column 5 Line 55 – 60: the ECM control word can be retrieved during replaying);

combining the retrieved items with decryption information with the stream during replay at times selected under control of the synchronization information (Kamperman : Column 8 Line 42 – 51, Column 7 Line 2 – 5 and Column 9 Line 21 – 26: a time-stamped message included in the ECM control word message to assure the CW is valid only until the age of viewing time is ended – i.e. the time-stamped validity period of the ECM control word decryption information).

As per claim 8, Kamperman teaches a conditional access apparatus for processing a broadcast data stream that contains a stream of encrypted data and a stream of messages (Kamperman : Column 1 Line 55 – Column 2 Line 3), data in successive segments of the stream of encrypted data being decryptable with successive decryption information from the messages (Kamperman : Column 1 Line 55 – 67: ECM messages), the apparatus comprising:

storage means, the apparatus being arranged to store the stream of encrypted data in the storage means (Kamperman : Column 2 Line 61 – 62), as well as storing items with decryption information for the encrypted data independently retrievable from the stream (Kamperman : Column 2 Line 59 – 61, Column 1 Line 55 – 67 and Column 4

Line 41 – 59: ECM message embedded / multiplexed with the encrypted / scrambled data that contains control word (CW) (i.e. decryption information) corresponding to reception of the data stream during each respective 10 seconds block of data), and storing synchronization information linking respective points in the stored stream of encrypted data to respective ones of the items with decryption information (Kamperman : Column 8 Line 42 – 51 and Column 7 Line 2 – 5: the time-stamped information is qualified as a synchronization information that determines the validity time period of the ECM control word (i.e. decryption information) that is used to successfully decode the encrypted data);

a replay unit for replaying a stored part of the stream of encrypted data (Kamperman : Column 5 Line 55 – 60: a play-back recorder);

a retrieval unit arranged to retrieve the items with decryption information for the points in said stored part from the storage means, and to feed said items to the replay unit during said replaying (Kamperman : Column 5 Line 55 – 60: the ECM control word can be retrieved during replaying);

a secure device, arranged to generate control words under control of the decryption information and to feed the control words to the replay unit to decrypt the items (Kamperman : Column 5 Line 31 – 41, Column 2 Line 40 – 41: a smart card);

a synchronization unit arranged to combine the retrieved items with decryption information with the stream during replay at times selected under control of the synchronization information (Kamperman : Column 9 Line 21 – 26: the time-stamped information is qualified as a synchronization information that determines the validity time period of the ECM control word (i.e. decryption information) that is used to successfully decode the encrypted data) by feeding the decryption information to the secure device at the selected times, for generating the control words (Kamperman : Column 2 Line 59 – 61 and Column 1 Line 55 – 67).

As per claim 2, Kamperman teaches during replay the stream is fed to a decoder and the decryption information is combined with the stream by feeding the decryption information to a secure device, which in response to the decryption information feeds control words to the decoder (Kamperman : Column 5 Line 31 – 41, Column 2 Line 40 – 41 and Column 9 Line 21 – 26: a smart card).

As per claim 3 and 9, Kamperman teaches storing the items with decryption information each in association with a respective time stamp value (Kamperman : Column 2 Line 59 – 61, Column 1 Line 55 – 67 and Column 4 Line 41 – 59: ECM message embedded / multiplexed with the encrypted / scrambled data that contains control word (CW) (i.e. decryption information) corresponding to reception of the data stream during each respective 10 seconds block of data); maintaining a progressive time value counter during replay of the stream (Kamperman : Column 2 Line 59 – 61 and Column 4 Line 41 – 59 : the ECM message contains the time-stamped message and data stream signal progresses as a function of time – i.e. time is divided into successive time intervals (e.g. every 10 seconds); where each time interval the encrypted data is encrypted based on the respective CW of its ECM message and data decoder needs a corresponding control word to decrypt the data from each time-interval respectively) and combining each particular retrieved item with the stream in response to detection that the time stamp counter reaches the time stamp value associated with the particular retrieved item (Kamperman : Column 9 Line 21 – 26 and Column 7 Line 2 – 5: a time-stamped message included in the ECM control word message to assure the CW is valid only until the age of viewing time is ended – i.e. the time-stamped validity period of the ECM control word decryption information).

As per claim 4 and 10, Kamperman teaches maintaining a further progressive time value counter during reception of the stream; sampling values from said further time value counter each time when a respective one of the messages is detected during reception (Kamperman : Column 2 Line 59 – 61 and Column 4 Line 41 – 59 : the ECM message contains the time-stamped message and data stream signal progresses as a function of time – i.e. time is divided into successive time intervals (e.g. every 10 seconds); where each time interval the encrypted data is encrypted based on the respective CW of its ECM message and data decoder needs a corresponding control word to decrypt the data from each time-interval respectively); storing decryption information from said message in the items with decryption information; storing the sampled value sample for each respective one of the messages as said time stamp value associated with the item that contains decryption information from said message (Kamperman : Column 2 Line 59 – 61, Column 8 Line 42 – 51 and Column 7 Line 2 – 5).

As per claim 5, Kamperman teaches the encrypted data contains time counting information used for controlling progress of the time value counter (Kamperman : Column 2 Line 59 – 61, Column 4 Line 41 – 59, Column 8 Line 42 – 51 and Column 7 Line 2 – 5: the scrambled data is stored with the associated ECM message that contains the time-stamped message and data stream signal progresses as a function of time – i.e. time is divided into successive time intervals (e.g. every 10 seconds); where each time interval the encrypted data is encrypted based on the respective CW of its ECM message and data decoder needs a corresponding control word to decrypt the data from each time-interval respectively).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 6 – 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kamperman (U.S. Patent 5,991,400), in view of Peterka et al. (U.S. Patent 2002/0170053).

As per claim 6, Kamperman teaches detecting respective ones of the messages detected during reception of the stream (Kamperman : Column 1 Line 55 – Column 2 Line 3 and Column 4 Line 41 – 59: ECM message embedded / multiplexed with the encrypted / scrambled data that contains control word (CW) (i.e. decryption information) corresponding to reception of the data stream during each respective 10 seconds block of data).

However, Kamperman does not teach expressly assigning different sequence numbers to the detected messages.

Peterka teaches assigning different sequence numbers to the detected messages (Peterka : Para [0123] Line 1 – 7: each of the ECM message can be assigned a sequence number to protect replay attack).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Peterka within the system of Kamperman because (a) Kamperman teaches, in a conditional access multimedia system, using a time-stamped information to associate the respective ECM message that contains the decryption information of control words during the play-back of the recorded stream (Kamperman : Column 8 Line 43 – 50) and (b) Peterka teaches providing a protection method against replay attack by using a sequence number that can corresponds to a time-stamped information of a respective ECM message / EMM message in a conditional access multimedia audio / video system (Peterka : Abstract and Para [0123] Line 1 – 7).

storing information representing the sequence numbers among the encrypted data at locations where the messages to which the sequence numbers have been assigned occurred in the stream during reception (Peterka : Para [0123] Line 1 – 7 & Kamperman : Column 8 Line 43 – 50 and Column 4 Line 41 – 59); storing each sequence number in association with a respective one of the items with decryption information that contains encryption information from the message to which the sequence number is assigned (Peterka : Para [0123] Line 1 – 7 & Kamperman : Column 9 Line 24 – 26); using the sequence numbers stored among the stream to retrieve and time the items associated with the sequence numbers (Peterka : Para [0123] Line 1 – 7 & Kamperman : Column 8 Line 43 – 50 and Column 4 Line 41 – 59).

As per claim 7, Kamperman as modified teaches the messages are stored at their original locations among the encrypted data, the sequence numbers being inserted in the messages during storage, the decryption information from the items associated with the sequence numbers inserted in the items being used when the messages are encountered during replay (Peterka : Para [0123] Line 1 – 7 & Kamperman : Column 8 Line 43 – 50 and Column 4 Line 41 – 59).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Primary Examiner, Art Unit 2131

Longbit Chai Ph.D.
Patent Examiner
Art Unit 2131
2/4/2008